18. Offensive vs Defensive Security

🛡️ Offensive vs Defensive Security

1. **What is Offensive Security?**

- **Offensive security** involves proactively identifying and exploiting vulnerabilities to improve system security.
- **Goal:** Simulate real-world attacks to **test defenses** and uncover weaknesses before malicious hackers do.
- Examples:
  - Penetration testing
  - Red team operations
  - Exploit development

2. **What is Defensive Security?**

- **Defensive security** focuses on **preventing, detecting, and responding** to cyber threats.
- Involves setting up **firewalls**, **IDS/IPS**, **patching**, **monitoring**, and **user awareness**.
- Examples:
  - Blue teaming
  - Security Operations Center (SOC)
  - SIEM systems

3. **How Do Red Teams Contribute to Cybersecurity?**

- Red teams simulate **realistic attacks** to test an organization’s security posture.
- They operate like real-world adversaries (stealthy, goal-oriented).
- Contributions:
  - Identify blind spots in detection
  - Help improve response plans
  - Pressure-test blue teams

4. **What is the Role of Blue Teams?**

- Blue teams are responsible for **defending systems** from attacks.
- Duties:
  - Monitor logs and alerts

    - Respond to incidents
    - Patch systems and harden defenses
    - Use tools like **SIEM**, **IDS**, **firewalls**

---

5. **What is a Purple Team in Cybersecurity?**

- **Purple teams** bridge the gap between red and blue teams.
- Purpose:
    - Ensure **collaboration and feedback** between offense and defense.
    - Share tactics and improve detection and response.
- It’s a **philosophy** or **function**, not a separate team in every case.

---

6. **What is Ethical Hacking?**

- Ethical hacking is the **authorized attempt** to bypass system security to find weaknesses.
- Also called **White-Hat hacking**.
- Done with permission and follows legal boundaries.
- Common certifications: **CEH**, **OSCP**

---

7. **What is Penetration Testing and Its Purpose?**

- Penetration testing (pentesting) is a controlled attack on a system to uncover vulnerabilities.
- **Purpose:**
    - Validate security controls
    - Discover exploitable weaknesses
    - Improve overall security posture

---

8. **What Are the Differences Between Vulnerability Assessment and Penetration Testing?**

Aspect	Vulnerability Assessment	Penetration Testing
Scope	Broad scan for flaws	Targeted attack simulation
Automation	Largely automated	Manual and automated
Depth	Shallow, many issues	Deep, fewer issues, with exploitation
Risk Confirmation	No exploitation	Exploits vulnerabilities
Goal	Identify and list risks	Show real-world impact

---

9. **What is the Cyber Kill Chain?**

A **framework by Lockheed Martin** describing the steps of a cyberattack:

1. **Reconnaissance**
2. **Weaponization**
3. **Delivery**
4. **Exploitation**
5. **Installation**
6. **Command & Control (C2)**
7. **Actions on Objectives**

👉 Helps defenders understand and disrupt attacks early.

---

10. How Do SIEM Systems Help in Cybersecurity Defense?

- **SIEM (Security Information and Event Management)** tools collect and analyze security logs.
- Helps in:
    - **Real-time alerting**
    - **Incident detection**
    - **Threat intelligence correlation**
    - **Forensics and reporting**

Popular SIEMs: **Splunk**, **ELK Stack**, **QRadar**, **AlienVault**

---

11. What Are Common Offensive Cybersecurity Tools?

- **Nmap** – Network scanning
- **Metasploit** – Exploitation framework
- **Burp Suite** – Web vulnerability testing
- **Wireshark** – Network traffic analysis
- **John the Ripper** / **Hashcat** – Password cracking
- **Gobuster/Dirb** – Content discovery
- **Hydra** – Brute-force attacks

---

12. What Are Common Defensive Cybersecurity Measures?

- **Firewalls**
- **Intrusion Detection/Prevention Systems (IDS/IPS)**
- **Anti-malware/antivirus**
- **Security patching**
- **Multi-factor authentication (MFA)**
- **Endpoint Detection and Response (EDR)**

- **SIEM monitoring**
- **Network segmentation**

13. How Does Threat Hunting Work in Cybersecurity?

- Threat hunting is the **proactive search** for signs of compromise in systems **before alerts are triggered**.
- Uses:
    - Threat intelligence
    - Behavioral analysis
    - Hypothesis-driven searches (e.g., based on MITRE ATT&CK)
- Tools: **SIEM**, **Sysmon**, **ELK Stack**, **Velociraptor**

14. What Are the Phases of an Incident Response Plan?

1. **Preparation** – Tools, training, policies
2. **Identification** – Detecting incidents
3. **Containment** – Short-term and long-term containment
4. **Eradication** – Removing the threat
5. **Recovery** – Restoring normal operations
6. **Lessons Learned** – Post-incident review to improve

15. Why Is Security Awareness Training Important for Organizations?

- **Human error** is a leading cause of breaches.
- Awareness training helps employees:
    - Spot phishing attempts
    - Practice secure password habits
    - Avoid social engineering traps
    - Follow security policies
- Reduces attack surface and supports a **security-first culture**.